CLAIMS

1. An encryption method for generating a ciphertext from divided plaintexts obtained by dividing a plaintext to be encrypted, comprising the steps of:

dividing a plaintext to be encrypted into a plurality of 1-bit divided plaintexts;

selecting one public key for each divided plaintext among two public keys which include therein a random number term and are prepared for each divided plaintext, according to a bit pattern of the plurality of divided plaintexts; and

generating a ciphertext by using the plurality of divided plaintexts and selected public keys.

2. The encryption method as set forth in claim 1, wherein the ciphertext is generated by adding a plurality of products of the respective divided plaintexts and correspondingly selected public keys.

3. The encryption method as set forth in claim 1, wherein the ciphertext is generated by multiplying and/or adding a plurality of product-sum terms obtained by adding a plurality of products of the respective divided plaintexts and correspondingly selected public keys.

4. The encryption method as set forth in claim 1, wherein the ciphertext is generated by using a result of operating multi-stage modular-transformation by a plurality

of random numbers on the selected public keys.

5. A cryptographic communication method for communicating information by a ciphertext between entities, comprising the steps of:

dividing at a first entity a plaintext to be encrypted into a plurality of 1-bit divided plaintexts;

selecting at the first entity one public key for each divided plaintext among two public keys which include therein a random number term and are prepared for each divided plaintext, according to a bit pattern of the plurality of divided plaintexts;

generating at the first entity a ciphertext by using the plurality of divided plaintexts and selected public keys and transferring the ciphertext to the second entity; and

decrypting at the second entity the transferred ciphertext into a plaintext.

6. A device for generating a ciphertext by using divided plaintexts obtained by dividing a plaintext to be encrypted and public keys, comprising:

a database storing two public keys including a random number term therein for each divided plaintext in advance;

a divider dividing a plaintext to be encrypted into a plurality of 1-bit divided plaintexts;

a selector selecting one public key for each divided plaintext among the two public keys, according to a bit

pattern of the plurality of 1-bit divided plaintexts; and

an encryptor generating a ciphertext by using the plurality of divided plaintexts and selected public keys.

7. A cryptographic communication system for communicating information by a ciphertext between entities, comprising:

an encryptor generating a ciphertext from a plaintext by using the encryption method of claim 1;

a communication path transmitting the generated ciphertext from a first entity to a second entity; and

a decryptor decrypting the transmitted ciphertext into a plaintext.

8. A computer memory product having computer readable program code means for causing a computer to generate a ciphertext by using divided plaintexts obtained by dividing a plaintext to be encrypted and public keys, said computer readable program code means comprising:

program code means for causing the computer to divide a plaintext to be encrypted into a plurality of 1-bit divided plaintexts;

program code means for causing the computer to select one public key for each divided plaintext among two public keys which include therein a random number term and are prepared for each divided plaintext, according to a bit pattern of the plurality of divided plaintexts; and

program code means for causing the computer to generate a ciphertext by using the plurality of divided plaintexts and selected public keys.

9. A computer memory product having computer readable program code means for causing a computer to decrypt a ciphertext generated by using a plurality of 1-bit divided plaintexts obtained by dividing a plaintext and a plurality of public keys selected in such a manner that one public key is selected for each divided plaintext among two public keys which include therein a random number term and are prepared for each divided plaintext, according to a bit pattern of the plurality of divided plaintexts, said computer readable program code means comprising:

program code means for causing the computer to sequentially decrypt the divided plaintexts while identifying the selected public keys.

10. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate a ciphertext by using divided plaintexts obtained by dividing a plaintext to be encrypted and public keys, comprising:

a code segment for causing the computer to divide a plaintext to be encrypted into a plurality of 1-bit divided plaintexts;

a code segment for causing the computer to select one

public key for each divided plaintext among two public keys which include therein a random number term and are prepared for each divided plaintext, according to a bit pattern of the plurality of divided plaintexts; and

a code segment for causing the computer to generate a ciphertext by using the plurality of divided plaintexts and selected public keys.

11. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to decrypt a ciphertext generated by using a plurality of 1-bit divided plaintexts obtained by dividing a plaintext and a plurality of public keys selected in such a manner that one public key is selected for each divided plaintext among two public keys which include therein a random number term and are prepared for each divided plaintext, according to a bit pattern of the plurality of divided plaintexts, comprising:

a code segment for causing the computer to sequentially decrypt the divided plaintexts while identifying the selected public keys.

12. An encryption method for generating a ciphertext from divided plaintexts obtained by dividing a plaintext to be encrypted, comprising the steps of:

dividing a plaintext to be encrypted into a plurality of s-bit (s: natural number) divided plaintexts;

selecting one public key for each divided plaintext among 2^s public keys which include therein a random number term and are prepared for each divided plaintext, according to bit data of each divided plaintext; and

generating a ciphertext by using the selected public keys.

13. The encryption method as set forth in claim 12, wherein the ciphertext is generated by adding the selected public keys.

14. The encryption method as set forth in claim 12, wherein the ciphertext is generated by multiplying and/or adding a plurality of sum terms obtained by adding the selected public keys.

15. The encryption method as set forth in claim 12, wherein the ciphertext is generated by using a result of operating multi-stage modular-transformation by a plurality of random numbers on the selected public keys.

16. A cryptographic communication method for communicating information by a ciphertext between entities, comprising the steps of:

dividing at a first entity a plaintext to be encrypted into a plurality of s-bit (s: natural number) divided plaintexts;

selecting at the first entity one public key for each divided plaintext among 2^s public keys which include therein

a random number term and are prepared for each divided plaintext, according to bit data of each divided plaintext;

generating at the first entity a ciphertext by using the selected public keys and transferring the ciphertext to a second entity; and

decrypting at the second entity the transferred ciphertext into a plaintext by the other entity.

17. A device for generating a ciphertext based on divided plaintexts obtained by dividing a plaintext to be encrypted and public keys, comprising:

a database storing 2^s (s: natural number) public keys including a random number term therein for each divided plaintext in advance;

a divider dividing a plaintext to be encrypted into a plurality of s-bit divided plaintexts;

a selector selecting one public key for each divided plaintext among the 2^s public keys, according to bit data of each divided plaintext; and

an encryptor generating a ciphertext by using the selected public keys.

18. A cryptographic communication system for communicating information by a ciphertext between entities, comprising:

an encryptor for generating a ciphertext from a plaintext by using the encryption method of claim 12;

a communication path transmitting the generated ciphertext from a first entity to a second entity; and

a decryptor decrypting the transmitted ciphertext into a plaintext.

19. A computer memory product having computer readable program code means for causing a computer to generate a ciphertext based on divided plaintexts obtained by dividing a plaintext to be encrypted and public keys, said computer readable program code means comprising:

program code means for causing the computer to divide a plaintext to be encrypted into a plurality of s-bit (s: natural number) divided plaintexts;

program code means for causing the computer to select one public key for each divided plaintext among 2^s public keys which include therein a random number term and are prepared for each divided plaintext, according to bit data of each divided plaintext; and

program code means for causing the computer to generate a ciphertext by using the selected public keys.

20. A computer memory product having computer readable program code means for causing a computer to decrypt a ciphertext generated by using a plurality of public keys selected in such a manner that one public key is selected for each of a plurality of s-bit divided plaintexts obtained by dividing a plaintext among 2^s (s: natural number) public

keys which include therein a random number term and are prepared for each divided plaintext, according to bit data of each divided plaintext, said computer readable program code means comprising:

program code means for causing the computer to sequentially decrypt the divided plaintexts while identifying the selected public keys.

21. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate a ciphertext based on divided plaintexts obtained by dividing a plaintext to be encrypted and public keys, comprising:

a code segment for causing the computer to divide a plaintext to be encrypted into a plurality of s-bit (s: natural number) divided plaintexts;

a code segment for causing the computer to select one public key for each divided plaintext among 2^s public keys which include therein a random number term and are prepared for each divided plaintext, according to be data of each divided plaintext; and

a code segment for causing the computer to generate a ciphertext by using the selected public keys.

22. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to decrypt a ciphertext generated by using

a plurality of public keys selected in such a manner that one public key is selected for each of a plurality of s-bit divided plaintexts obtained by dividing a plaintext among 2^s (s: natural number) public keys which include therein a random number term and are prepared for each divided plaintext, according to bit data of each divided plaintext, comprising:

a code segment for causing the computer to sequentially decrypt the divided plaintexts while identifying the selected public keys.